INSS Insight No. 1112, December 17, 2018

Iran's Cyber influence Campaign against the United States, and Implications for Israel's Security

Itay Haiminis

Over the past six months, cyber security firms and technology companies have exposed extensive Iranian cognitive-related activity in cyberspace aimed primarily at the American public, with Iran's seeking to exacerbate internal US debates between different social groups. Iran's influence efforts in cyberspace reflect the importance Tehran attributes to the ideological struggle at home and against its external enemies, first and foremost the United States. In the regime's eyes, the United States, in addition to its political and economic war, is waging an ideological struggle for the hearts and minds of the Iranian public against the values of the Islamic Revolution. Therefore, Iran's cyber influence campaign is not merely a counteraction to US moves (real and imagined), but also another step in Iran's longstanding desire to destabilize the United States by weakening its internal robustness. Israel, likewise a target of Iranian cyber influence efforts, would do well to monitor Iran's developing cyberattack capabilities, along with Iran's overt threatening capabilities in conventional and non-conventional weapons.

In recent months, the increasingly tense relations between Tehran and Washington have been manifested again in cyberspace. Over the past six months, cyber security firms and technology companies have exposed extensive Iranian cognitive-related activity in cyberspace aimed primarily at the US public. Fire-Eye Ltd., a cyber security company, issued a warning about many fake news sites and profiles on Facebook and Twitter that in its assessment were operated by the Iranian regime as part of its cyber influence campaign. Cyber influence efforts were also exposed by Twitter, which posted one million Tweets generated by fake accounts; Facebook, too, announced it had deleted dozens of fake profiles.

These revelations come on the heels of other warnings regarding Iranian activity in cyberspace appearing in annual summaries published in November 2018 by Fire-Eye and Fortinet, another cyber security outfit, and a current study released by the US think tank Foundation for the Defense of Democracies. These publications all describe Iran as an increasingly aggressive player in cyberspace.

Contents and Methods

Iran's cyber influence efforts aim to exacerbate internal US debates between different groups (liberals versus conservatives, African-Americans versus Caucasians, Trump opponents versus Trump supporters). Typical examples of sensitive, charged issues in the United States are racism, Trump's controversial policies, and police brutality. Material on these issues was delivered so as to inflame passions and radicalize positions. Contents dealing with the Middle East were highly critical of US policy, Israel, and Saudi Arabia, compared to sympathetic coverage of Iran on developments in Yemen, Lebanon, Syria, and Iraq. It appears that in this context, Iran relies on its experience during the Obama administration when according to some US media elements, Iran was a possible partner in US efforts in the Middle East against radical Sunni Islam, with emphasis on the war against the Islamic State (ISIS) in Iraq.

To conceal its fingerprints while expanding the incitement circles, Iran has developed a broad synchronized network of fake but reliable-sounding news sites and social media identities, involved them in internet and social media discourse, and paid for their advertising. Furthermore, the contents are formulated in a way that speaks to the mindset of the target audiences. Still, Iran's efforts have not been foolproof. Use of Iranian contact data (such as phone numbers and email addresses), copied content, and poor writing have led to their public exposure. Until then, however, Iran managed to reach many people in the United States; some contents were viewed by millions of views, and some contents earned responses by hundreds of thousands of surfers.

Implications for Israel's Security

Iran's influence efforts in cyberspace reflect the importance Tehran attributes to the ideological struggle at home and against its external enemies, first and foremost the United States. In the regime's eyes, the United States, in addition to its political and economic war, is waging an ideological struggle for the hearts and minds of the Iranian public against the values of the Islamic Revolution. Therefore, Iran's cyber influence campaign is not merely a counteraction to US moves (real and imagined), but also another step in Iran's longstanding desire to destabilize the United States by weakening its internal robustness.

Like other states (including the United States, Russia, and China), Iran is proving it can reach large audiences, retain the covert nature of its efforts over long periods of time, and "infect" the public discourse with provocative content. In the future, this Iranian activity may prove to have made a decisive contribution to the erosion of trust in the media among US citizens, or led to a change in political and/or social positions. Moreover, Iran presumably benefits from the exposure of its activities, because despite the embarrassment involved, Iran has not suffered any consequences, and may even have managed to inflate the image of its intelligence and technology capabilities. In addition,

compared to past Iranian cognitive campaigns, the current activity demonstrates that Iran has improved its technological infrastructures and operational capabilities in both scope and quality (e.g., software mimicking human users).

Exposure in the media seems to have been made possible thanks to increased cooperation among technology companies, information security companies, and Western intelligence agencies. Such cooperation can be expected to become necessary over the next few years to confront cyber influence efforts of this type. For Israel's public and decisionmakers, these exposures make it possible to learn – in a way that to date was impossible – about yet another tool in Iran's operational toolbox.

It appears that Iran's cyber influence threat against Israel is still limited. In the past, Iran's cyber influence efforts against Israel, which amounted to website destruction and false contents planted in news sites, resulted in little significant public impact. Iran's news website directed at the Israeli public, recently exposed by Clear Sky Ltd., seems to have failed to influence the Israeli discourse. Furthermore, an examination of Iran's cyber influence efforts against Israel compared to Iran's other cyber influence efforts at this time suggests that Israel is not a central target. Iran's focus on other arenas may stem from the fact that Hezbollah is already engaged in cognitive efforts, whether via Nasrallah's threatening speeches or by way of the many media options at Hezbollah's disposal.

Nonetheless, looking ahead, one could sketch out several more severe scenarios of Iran turning its cyberspace influence tools against Israel. Iran might succeed in planting fake news items about impending Israeli attacks, to cause public panic and/or temporarily disrupt Israel's decision making process. Similarly, Iran might succeed in planting items that could convince an enemy state or terrorist organization of an intended Israeli attack, which in turn sparks a preemptive attack against Israel. In December 2016, Iran succeeded in eliciting a Pakistani verbal response to a false report that Israel had threatened Pakistan with a nuclear attack should Pakistan send forces to Syria.

Given the current features of Iran's influence effort in cyberspace, Israel would do well to monitor Iran's developing cyberattack capabilities (e.g., attacks on critical infrastructures or weapon systems), along with Iran's overt threatening capabilities in conventional and non-conventional weapons. As it confronts Iran's influence campaign in cyberspace, Israel must focus mostly on defensive measures, including exposure and disruption of Iranian efforts. Beyond this, Israel should leverage the exposure and disruption of Iran's influence tactics in cyberspace to attain political benefits by presenting these as yet another manifestation of Iran's negative regional conduct and violations of international norms.